ISBN 978-602-14917-7-5
The First International Conference of Food and Agriculture

COLLABORATION OF MQTT PROTOCOL AND VPN TUNELLING ON WEB-BASED SMART HOME MONITORING SYSTEM

Bekti Maryuni Susanto[1], Ery Setiyawan Jullev[2],
Department of Information Technology, PoliteknikNegeriJember

bekti@polije.ac.id[1], ery@polije.ac.id[2],

Abstract. Internet of Things or commonly known as IoT is one of the smart technologies that combine the environment with devices through internet media. Interoperability is a product or system characteristic, whose interface is truly understood, works with other products or systems. Therefore, a stable and lightweight data acquisition and data transmission mechanism is needed, one of which can be used is the Representational State Transfer (REST) mechanism that uses Unique Resource Identifiers (URIs), but REST is still unable to handle interoperability of each device, therefore an additional protocol is needed that can handle this, one of the most frequently used is Message Queue Telemetry Transport (MQTT). The use of REST and MQTT has weaknesses in security, data sent using REST and MQTT are able to be analyzed and retrieved data content using sniffing techniques. One technique that can be used to secure communication channels on the Internet of Things network is by utilizing a Virtual Private Network (VPN). This research applies OpenVPN to secure communication channels between Gateway IoT and Server. Network performance is measured using throughput and packet loss parameters. The measurement results show a throughput value 1004 bps and packet loss 0%.

Keywords : Internet Of Thing,REST, VPN,MQTT

1. Introduction

Internet of Things or commonly known as IoT is one of the smart technologies that combine the environment with devices through internet media. The use of IoT is growing in a short time, this is due to the development of information technology[1]. Based on a survey that was carried out by gartner in 2020 as many as 20 billion objects will be connected between one another [2]. This causes the involvement of many devices that are interconnected with sensors installed in the environment. So that with the existence of many devices it causes interoperability problems from each tool. Interoperability is a characteristic of a product or system, whose interface is truly understood, working with other products or systems, now or in the future, both in implementation and access, without any limitations[3].

To overcome this, a gateway or protocol is needed to bridge the interoperability. One of the tasks of the Gateway or protocol is to be able to handle interoperability issues and be able to handle requests and device profiles from each connected sensor or device.

One technology that is often used in dealing with these problems is the Device Profile for web services (DPWS) and Universal Plug and play (UPnP) which the DPWS itself adopts technology from the Web Service Definition Language (WSDL) [4], but DPWS itself has weaknesses that are difficult to implement, especially on devices with ARM architecture such as Arduino. Arduino itself is one of

the open source hardware platforms that can be developed and supports many interfaces such as zigbee, Ethernet, Bluetooth or other.

Therefore, a stable and lightweight data acquisition and data transmission mechanism is needed, one of which can be used is the Representational State Transfer (REST) mechanism that uses Unique Resource Identifiers (URIs), but REST is still unable to handle interoperability of each device, therefore an additional protocol is needed that can handle this, one of the most frequently used is Message Queue Telemetry Transport (MQTT).

MQTT itself is a machine to machine (M2M) connectivity protocol designed to transmit data very lightly using TCP / IP architecture [5]. The MQTT itself has the advantage of being able to transmit data with light bandwidth, low electricity consumption, very high latency and connectivity, availability of many variables and guaranteed negotiable data delivery [6].

However, using REST and MQTT has the disadvantage of security, the data sent using REST and MQTT can be analyzed and retrieved the data content using sniffing techniques. Sniffing itself is a data acquisition technique on a computer network by utilizing a packet that passes through the network and unpacks the package using certain techniques.

One technique that can be used to secure communication channels on the Internet of Things network is by utilizing a Virtual Private Network (VPN). VPN itself is a technology that allows users to use a private tunnel to transmit data over the internet so that data can be better protected [7].

Considering the problems regarding IoT, this study aims to collaborate between the MQTT protocol and VPN on monitoring smart home so that better security guarantees can be obtained for IoT implementation. In MQTT, a data transmission mechanism is needed to use the internet network using TCP / IP protocol. While on the VPN is used to secure the data transmission path to the server or other device

2. Literature Review

Literature review that will be used for this research are

2.1. Internet Of Things

Internet of Things (IoT) is a concept where internet connectivity can exchange information with each other with objects around it [1]. Many predict that the Internet of Things (IoT) is "the next big thing" in the world of information technology. This is because a lot of potential can be developed with the Internet of Things (IoT) technology.

2.2. MQTT Protocol

Message Queuing Telemetry Transport (MQTT) is a client server that publishes / subscribe. A lightweight, open and simple protocol, designed to be easy to implement. These characteristics make the MQTT usable in many situations, including its use in machine-to-machine (M2M) and Internet of Things (IoT) communications, this protocol runs on TCP / IP [2].

The MQTT protocol requires transportation that runs the MQTT command, the byte stream from the client to the server or the server to the client. The transport protocol used is TCP / IP. TCP / IP can be used for MQTT, besides TLS and WebSocket can also use TCP / IP. Connectionless networks such as the User Datragram Protocol (UDP) cannot be used because they can result in data reorder [8].

2.3. Virtual Private Network.

Virtual Private Network or better known as VPN is a private network created by utilizing public networks, or in other words creating a new WAN network that is separated physically and logically but is still able to form a single network.

Data packages that flow between sites and remote users will be encrypted and authenticated, thus ensuring data security, integrity and validity (RSA Security, 2003).VPN is widely used to improve the security of confidential communication data. In principle, a VPN is a communication connection that is personal and is done virtually. In simple terms, this VPN can be seen as making personal data communication lines on public internet networks.

3. Working Methodology

3.1. Requirement Engineering

Based on the problems in this study, engineering requirements are performed which function to determine the system requirements to be developed. The need for a web-based home lighting monitoring system using MQTT is shown in Figure 5. In Figure 5, a home lighting monitoring system requires an Internet of Things (IoT) gateway device to use Raspberry Pi that is connected to an OpenVPN server. So that website monitoring can be accessed from anywhere. Every house lamp is connected to a relay that is controlled via Raspberry GPIO pins.

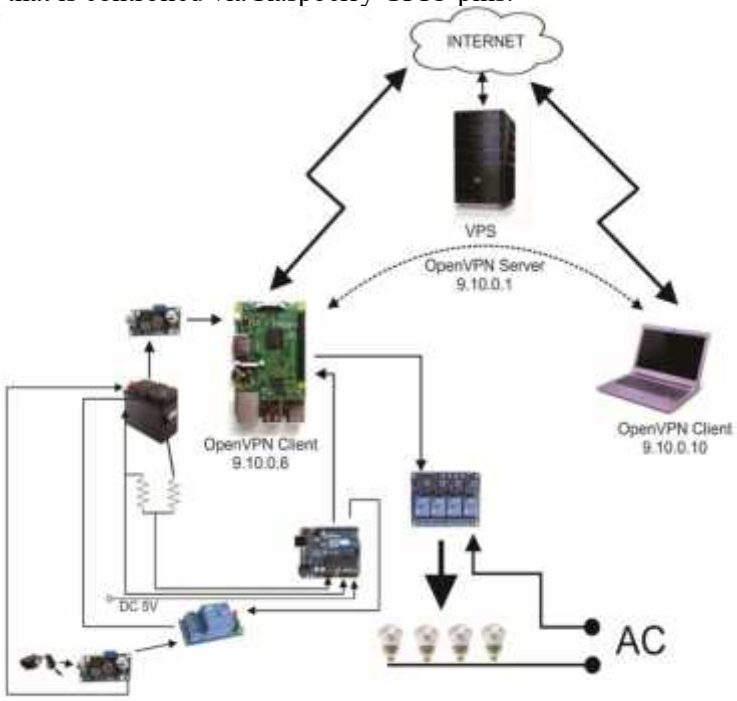

Figure 1 System requirements that will be developed

3.2. Data Analysis

This study uses the waterfall method, which consists of the requirements of engineering, design and implementation, testing, release and maintenance stages [8]. The research method used is experimental research. Experimental research is conducted where research involves investigating a causal relationship using tests controlled by researchers [9].

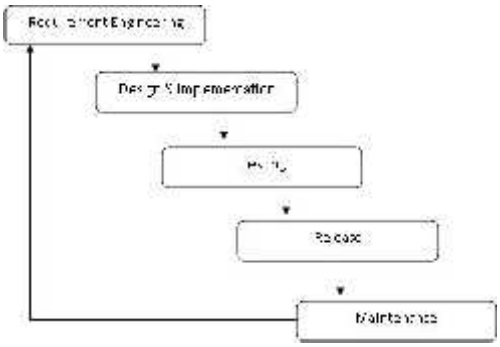

Figure 2 Flowchart system

The proposed smart home monitoring system uses the website as a user interface. Gateway smart home uses a single board computer device Raspberry Pi 3. This device has limited resources to be

accessed directly on a public network. Because a device that can be accessed directly on a public network requires a security mechanism to avoid security breaches. For this reason, this research proposes a mechanism to secure communication channels between users and smart home gateways using Virtual Private Network (VPN). By utilizing this VPN, the smart home gateway can be accessed by certain users who have the authorization to access it from anywhere and anytime. VPN makes the smart home and user gateways reside on a local network on the Internet network through a tunnel. The smart home gateway is in charge of communicating with smart devices using the Message Queue Telemetry Transport (MQTT) protocol. The smart home monitoring system is web-based with the collaboration of the mqtt protocol and the VPN connection shown on Figure 3.

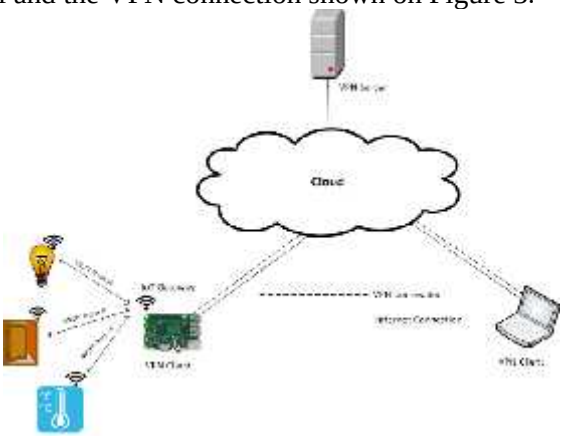

Figure3. Scenario ForVPN Access

4. Experiment and Result

Some sensors are used for data acquisition. These sensors are temperature and humidity sensors, PIR sensors, gas sensors and fire sensors. A microcontroller is connected directly with each sensor. This microcontroller is responsible for processing sensor data and forwarding the sensor data to the IoT gateway using the MQTT communication protocol. Then the data is stored on the Mysql database.. The following are the final results of the tools that created in figure 4:

Figure 4. Interface Program

Testing of sending data from nodemcu to raspberry pi starts from reading analog data received from sensor sensors. The sensor data is given a range then the range results are divided into two, namely 0 and 1. Then the data is sent using mqtt. In testing the data transmission from the mqtt broker to this database we can see the data data sent from the mqtt client to the mqtt broker namely the gas sensor data, the fire sensor, the 11 dht sensor and the pear sensor.

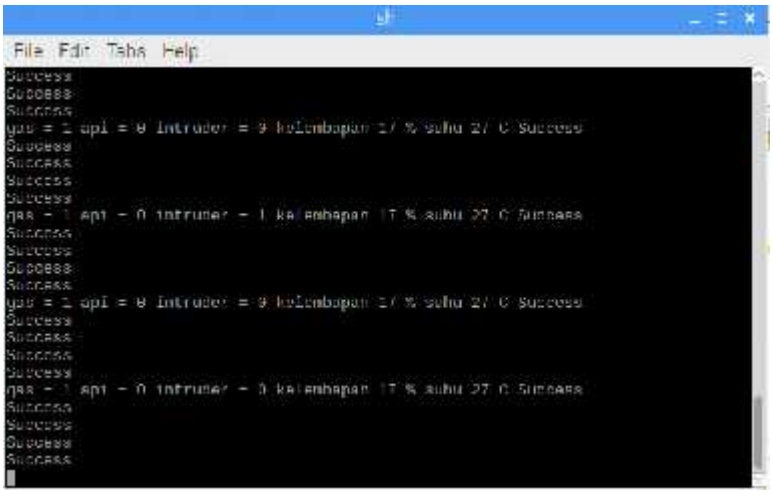

Figure 5. Data Exchange

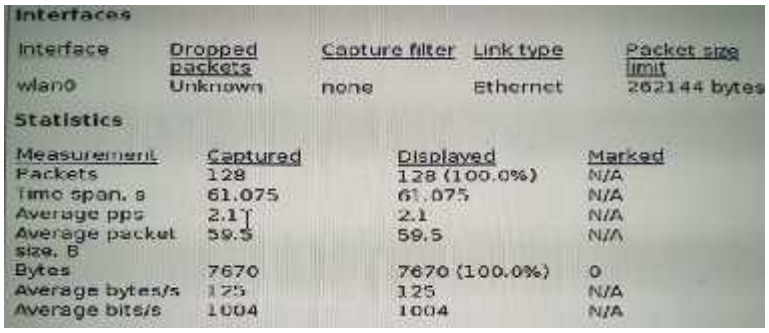

Figure 6. Throughput Exchange

Throughput measurement results show that the MQTT is able to transmit data using a fairly small bandwidth, which is equal to 1004 bps or less than 1 Kbps

5. Conclusion

Based on the problems that exist in the identification of the quality of cocoa fruit maturity, the following conclusions:

1. The MQTT protocol uses a small enough bandwidth to transmit data from the MQTT client to the MQTT server..
2. Control of the lights and doors of the house utilizing the control logic 1 and 0 sent by Raspberry through GPIO pins that are connected directly to the relay module.
3. Transmission of sensor data to Raspberry using the MQTT protocol which consists of two main components, namely nodemcu which is directly connected to the sensor as the MQTT client and Raspberry as the MQTT server.

Acknowledgments

Our thank goes to Department of Information Technology, PoliteknikNegeriJember, who has helped support for this research.